

How to Cooperate Locally to Improve Global Privacy in Social Networks?

On Amplification of Privacy Preserving Data Aggregation

Krzysztof Grining
Department of Computer Science
Faculty of Fundamental
Problems of Technology, WUT

Marek Klonowski
Department of Computer Science
Faculty of Fundamental
Problems of Technology, WUT

Malgorzata Sulkowska
Department of Computer Science
Faculty of Fundamental
Problems of Technology, WUT

1

Abstract—In many systems privacy of users depends on the number of participants applying collectively some method to protect their security. Indeed, there are numerous already classic results about revealing aggregated data from a set of users. The conclusion is usually as follows: if you have enough friends to “aggregate” the private data, you can safely reveal your private information.

Apart from data aggregation, it has been noticed that in a wider context privacy can be often reduced to being hidden in a crowd. Generally, the problems is how to create such crowd. This task may be not easy in some distributed systems, wherein gathering enough “individuals” is hard for practical reasons.

Such example are social networks (or similar systems), where users have only a limited number of semi trusted contacts and their aim is to reveal some aggregated data in a privacy preserving manner. This may be particularly problematic in the presence of a strong adversary that can additionally corrupt some users.

We show two methods that allow to significantly amplify privacy with only limited number of local operations and very moderate communication overhead. Except theoretical analysis we show experimental results on topologies of real-life social networks to demonstrate that our methods can significantly amplify privacy of chosen aggregation protocols even facing a massive attack of a powerful adversary.

We believe however that our results can have much wider applications for improving security of systems based on locally trusted relations.

Index Terms—anonymity, random graph, big component, adversary

I. INTRODUCTION

Most algorithms providing anonymity or privacy in distributed systems consist in hiding an element in a group of other elements. Indeed, one of the very first definitions of anonymity from [1] describes it as a *state of being not identifiable within a set of subjects, the “anonymity set”*.

Similar approach to privacy in the context of data bases is caught in *k-anonymity* metrics ([2], [3], [4]). That is, the privacy is preserved as long as each element is revealed in a group of at least *k* other, identical elements. In this metric as well as some consecutive concepts like *ℓ-diversity* [5] or *m-invariance* [6], the bigger the “anonymity set” is, the stronger the privacy guarantees are. This idea is also reflected in further definitions of anonymity/privacy [7], [8].

It turns out however that similar phenomenon can be also observed in systems typically investigated from *differential privacy* perspective. Let us remind that this privacy metric is in fact a standard one and was introduced in the seminal paper [9]. In the context of distributed system of somehow connected individuals we usually consider a problem where some function of data has to be revealed preserving privacy of individuals. Many real life cases fall into this scenario. The most obvious example is privacy preserving data aggregation, wherein we need to reveal e.g. a sum of values of users protecting their

privacy at the same time. Such aim can be realized using combination of cryptography and the common trick of adding random value, (*a noise*), to the aggregated data (see for example [10] and [11]). It turns however that the bigger the set of individual contributed to the sum, the less noise has to be added to protect privacy of individuals. Alternatively, having the same level of privacy one can reveal more exact statistics if they refer to a bigger set of individuals.

In our paper we consider a distributed system that consists of nodes (individuals having some local, possibly sensitive, data) with connections constituting a graph modeled as a preferential attachment process. This model is believed to be appropriate for a wide spectrum of real systems including social networks. We may assume that each individual has a very constrained knowledge about the network limited to some (**semi**)trusted neighbors. We formally prove that using a simple algorithm (adding some extra connections between nodes) one may protect privacy of nodes even in the presence of an adversary capable of corrupting significant number of nodes. What is more important, our algorithm needs only some moderate number of **local** operations. In particular, the exact topology or even its exact size may remain unknown. Apart from rigid formal analysis we provide experimental results performed on data from real networks.

In Section II we present a general model with adversary. In Section III we present our distributed protocols which may be used to enhance privacy (e.g. in social networks). In Sections IV and V we provide analytic and experimental analysis of our protocols. In Section VI we show two examples of privacy amplification using our generic method. Then in Section VII we present some related papers and finally in Section VIII we conclude and outline some interesting problems for future work.

II. GENERAL ADVERSARIAL MODEL

We consider a social network represented as a graph *G*. The nodes and edges of *G* represent users and friendship relation between pairs of them, respectively.

Our model can be directly used for other distributed systems, wherein a privacy preserving data computation problem is considered (e.g., a sensor network or a systems of smart meters) as long as some assumptions typical for social networks about the network topology are fulfilled.

The intuition behind our adversarial model is as follows. We assume that the Adversary can corrupt some of the users. Corruption gives the Adversary control over the node, yet we assume that he is an honest-but-curious type of Adversary. Namely, corrupted nodes follow the protocol, but they are trying to learn information about processed data and share all information they have with the Adversary.

¹Supported by Polish National Science Center - NCN, decision number DEC-2013/ 08/M/ST6/00928 (Harmonia)

The corruption of nodes can either be done in a random way or the Adversary can choose an arbitrary subset of nodes to corrupt, knowing the exact structure of the graph (say, he may attack the nodes with the highest degree). Note that random corruptions can model scenario when some users install protecting software and others remain attack-prone. This case also covers the situation with unexpected failures, without an actual presence of Adversary.

Note that the Adversary has full access to all information processed by corrupted nodes. As we show later, from the perspective of the Adversary all connections incident to a corrupted node are removed from the graph G .

Definition 1: We will say that a graph is ξ -strong if a subgraph induced by its honest nodes has largest connected component of size at least ξn , where n is the number of honest nodes.

Clearly, corruption of a significant number of nodes can dramatically decrease the ξ -strength. For prevention, we can enrich the graph by adding some edges between users, e.g., between some arbitrary user and a friend of his friend. For practical reasons all these operations need to be **local** (no global topology is known) and simple.

We formally define *Disconnection Game* with Adversary \mathcal{A} and a distributed protocol \mathcal{P} as follows. We have a network with underlying undirected graph $G = (V, E)$ This can either be a specific real network graph or e.g., a randomly generated scale-free graph. We define Disconnection Game, denoted by $\mathcal{DG}(G, \mathcal{A}, \mathcal{P})$ in the following way:

- 1) \mathcal{P} : the set of edges E is enriched by adding edges chosen between pairs of unconnected nodes. Rules of adding edges depend on specific game instantiation. This resulting graph is denoted $G_P = (V, E \cup E_P)$, where E_P is the set of edges added after \mathcal{P} was applied.
- 2) The Adversary chooses, according to restrictions in this game instantiation, a subset C of nodes. The nodes belonging to C are *corrupted* and removed from the graph with their incident edges denoted by E_C . Note that the Adversary knows only the initial graph G .
The resulting graph is denoted $G_A = (V \setminus C, (E \cup E_P) \setminus E_C)$. We assume that C does not depend on the set E_P . This assumption reflects the assumption that the adversary does not know choices of uncorrupted nodes.
- 3) The outcome of the game is the fraction of nodes belonging to the biggest connected component in graph G_A .

The model presented in this section is a problem of robustness of the network (see for example [12], [13], [14], [15]). It is, however, worth mentioning that, unlike previous papers in that field, we require that the enhancing protocol is done in a distributed way and without much knowledge of global topology of the graph. Moreover, we pick rather strong notion of robustness, namely the size of the largest connected component.

If the resulting structure is ξ -strong, it means that there exists a structure that is **not** controlled by the adversary that is connected and contains at least $\xi \cdot n$ out of n nodes. Intuitively, this allows to provide a common response secured in such way that the adversary cannot observe separate inputs of nodes but the aggregated value of a large set of nodes. In Section VI we present references to particular protocols.

III. SECURITY-ENHANCING PROTOCOLS

We present two protocols aimed at improving ξ -strength of the network and in consequence security of aggregation protocols. We prove their properties both in analytic (Sec. IV) and experimental (Sec. V) way for underlying graphs typical for social networks.

A. m -Two Steps Friend Finder

The person who wants to improve his chances of being in the big component asks his friend (chosen uniformly at random) to recommend him yet to another friend. Namely, our new friend is a former "friend of a friend" that is added to the list of connections (or just a separated contact used for privacy-preserving actions). This procedure is iterated m times, namely ask m randomly chosen friends for recommendations. That would result in obtaining (at most) m new friends. Note that sometimes it might happen that a specific "friend of a friend" will be recommended more than once.

Formally, every node that wants to actively participate in the protocol performs a random walk of length 2 starting from himself. Note that one could propose different length of the random walk, our choice of length 2 is to minimize communication and keep the protocol as local as possible.

Formally the m -Two Steps Friend Finder (m -2SFF, for shortness) is presented as an Algorithm 1.

```

1 foreach node  $v$  do
2   for  $m$  times do
3     1. Choose node  $w$  uniformly at random from  $N(v)$ .
4     2. Query  $w$  to get id of its neighbor.
5     3. Node  $w$  chooses  $u$  uniformly at random from  $N(w)$  and
6       sends its id to  $v$ .
7     4. Create edge  $(v, u)$ .
```

Algorithm 1: m -2SFF

Note that m -2SFF can be performed by a node without any knowledge of the underlying graph, except its neighbors. Moreover, it can be done in a fully distributed manner, with $O(mn')$ messages sent in the network, where $n' \leq n$ is the number of nodes participating in the protocol.

B. m -Ask Fat For a Friend

The approach in this protocol is substantially different. Here we want to rely on the preferential attachment properties of real networks. In particular, we assume that there is a commonly known list of a few nodes with highest degrees. We will call them *fat nodes*. In real life situation we might think that there are a few well-known and somewhat trusted parties in the distributed system.

Existence of such fat nodes is typical for structures governed by preferential attachment model (a.k.a. "rich get richer"). Note that there is a vast research in this kind of models and it turns out that complex, real life networks tend to exhibit such properties.

m -Ask Fat For a Friend (m -A3F) goes as follows. Every node that wants to improve its chance to belong to the big component has to choose uniformly at random one fat node from the common list and ask for an address of one of its neighbors chosen at random. Formally, m -A3F protocol is presented in Algorithm 2 and 3.

```

1 foreach node  $v$  do
2   for  $m$  times do
3     1. Choose node  $w$  at random from the common list of fat
4       nodes .
5     2. Query  $w$  to get id of its neighbor.
6     3. Node  $w$  chooses  $u$  uniformly at random from  $N(w)$  and
       sends its id to  $v$ .
7     4. Create edge  $(v, u)$ .
```

Algorithm 2: m -A3F (code for a regular node)

Using a list of 'fat' nodes may be perceived as a bottleneck of the protocol, yet one should easily realize that in many real life cases the

```

1 foreach fat node  $w$  do
2   if queried by node  $v$  then
3     Reply with  $u$  chosen at random from  $N(w)$ .

```

Algorithm 3: m -A3F (code for a fat node)

fat node has significantly more resources. Think about the case where the network is the WWW and 'fattest' nodes are e.g., Google, Yahoo or Facebook. Moreover a fat node does not participate in further communication. It just contacts two nodes so that they can establish an independent connection.

In the next Sections we show that using fat nodes for finding friends substantially improves the immunity of the graph even facing a massive attack of the adversary.

IV. ANALYTIC RESULTS

In this Section we analyse a specific, most interesting case of our protocols in a general model. Other cases are also considered in the next Section. Let us analyse the $\log n$ -A3F with Adversary knowing the topology of graph G in advance thus attacking the nodes with the highest degree. We consider $G = (V, E)$ to be preferential attachment graph having some properties that can be met in real-life networks. One of such properties is existence (whp) of a group of vertices having high (in some sense) degrees. Their neighborhood covers whp the linear number of vertices from V .

Thus, let us assume throughout this Section the following. Let $W \subset V$ be the subset of vertices whose degrees vary from $an/\log n$ to $bn/\log n$ for some constants a, b , $|W| = C \log n$ for some constant C . W is the set of the fat nodes from our protocol and, at the same time, the set of vertices that will be corrupted by Adversary. By N_W we denote the neighborhood of W without vertices from W , thus $N_W = \bigcup_{i=1}^{|W|} N(w_i) \setminus W$, where $N(w_i)$ is the neighborhood of w_i . We assume also that $|V \setminus (W \cup N_W)| = \alpha n$ for some constant $0 < \alpha < 1$. Let $V_\alpha = V \setminus (W \cup N_W)$. We will use the well known fact about the Erdős-Renyi $G(n, p)$ model (see for example [16]), namely that whenever $p \geq (1 + \varepsilon) \log n/n$ for some $\varepsilon > 0$, then whp $G(n, p)$ is connected.

First, let us consider the case in which all vertices want to participate in the $\log n$ -A3F Protocol.

Theorem 1: If $Ca < 1 - \alpha$ then after executing $\log n$ -A3F for all vertices in $G = (V, E)$ we obtain $G_A = (V \setminus W, (E \cup E_P) \setminus E_C)$ which is whp 1-strong. (Recall that E_P is the set of edges added during the protocol execution and E_C is the set of edges incident to vertices from W .)

Proof. Note that the set of vertices of G_A satisfies $V \setminus W = N_W \cup V_\alpha$ and N_W and V_α are disjoint. First, let us concentrate on the set N_W . Let $u, v \in N_W$. Let i be such that $\{w_i, v\} \in E$. Let us estimate the probability that there exists an edge $\{u, v\}$ (denote this event by $[u \leftrightarrow v]$). Let $[u \rightarrow v]$ denote the event that u established an edge $\{u, v\}$ during the protocol. For some $\varepsilon > 0$ and sufficiently big n we get

$$\begin{aligned}
\mathbb{P}[u \rightarrow v] &\geq 1 - \left(1 - \frac{1}{C \log n \deg(w_i)}\right)^{\log n} \geq \\
&1 - \left(1 - \frac{1}{C \log n} \frac{\log n}{an}\right)^{\log n} \geq \\
&1 - e^{-\frac{\log n}{Can}} \geq \frac{\log n}{Can + \log n} \geq (1 + \varepsilon) \log(|N_W|)/|N_W|.
\end{aligned} \tag{1}$$

Note that $1/(C \log n \deg(w_i))$ is the lower bound for the probability that v establishes an edge $\{v, u\}$ in a single step of the protocol.

Indeed, w_i does not need to be the only neighbor of u in W . The second inequality follows from the bounds for $\deg(w_i)$. The third inequality follows from the fact that $(1 - 1/x)^x$ converges to $1/e$ from below for $x > 0$, the fourth one from the fact that $e^x \geq 1 + x$. The last inequality follows because $Ca < 1 - \alpha$ and $|N_W| = (1 - \alpha)n - C \log n$. Since each vertex creates new edges during the protocol independently from other vertices, we have $\mathbb{P}[u \leftrightarrow v] = \mathbb{P}[u \rightarrow v] + \mathbb{P}[v \rightarrow u] - \mathbb{P}[u \rightarrow v] \mathbb{P}[v \rightarrow u]$. Of course, the lower bound (1) is true also for $\mathbb{P}[v \leftrightarrow u]$ for all $u, v \in N_W$. We can think that the subgraph of G induced on N_W (denote it by $G(N_W)$) decomposes into Erdos-Renyi $G(N_W, p)$, where $p \geq (1 + \varepsilon) \log(|N_W|)/|N_W|$, and some other random graph. Thus $G(N_W)$ will inherit some monotone properties of $G(N_W, p)$, among others, it will be connected whp. Since Adversary corrupts the nodes with the highest degrees, namely the whole set W , all the vertices from N_W will stay in G_A . Thus we have proved the existence (whp) of a giant component (which contains $G(N_W)$) of size at least $|N_W| = (1 - \alpha)n - C \log n$ in G_A .

Now, let us concentrate on the set V_α . Let us estimate the probability that a vertex $v \in V_\alpha$ is not connected with $G(N_W)$ (denote this event by $[v \not\leftrightarrow G(N_W)]$). What needs to happen is that whenever the fat node sends to v the id of u , u needs to be a fat node as well. Since there are $C \log n$ fat nodes and their degrees are at least $an/\log n$, we obtain

$$\mathbb{P}[v \not\leftrightarrow G(N_W)] \leq \left(\frac{1}{C \log n} \frac{C \log n}{an/\log n}\right)^{\log n} = \left(\frac{\log n}{an}\right)^{\log n}.$$

Vertices from V_α act during the protocol independently and the above probability is so small that we can simply estimate the probability that all vertices from V_α are connected with $G(N_W)$ (denote this event by $[V_\alpha \leftrightarrow G(N_W)]$) and show that it happens whp:

$$\mathbb{P}[V_\alpha \leftrightarrow G(N_W)] \geq \left(1 - \left(\frac{\log n}{an}\right)^{\log n}\right)^{\alpha n} \xrightarrow{n \rightarrow \infty} 1.$$

Thus whp G_A is connected. \square

The above theorem gave us a very strong result however its assumption about the number of vertices taking part in the protocol was also very strong. Now, let us discuss the following case: β fraction of vertices from V_α and γ fraction of vertices from N_W take part in the protocol. (We don't care about vertices from W because they are going to be corrupted and their incident edges will not appear in G_A eventually).

Theorem 2: If $Ca < 1 - \alpha$ and $Cb > \gamma(1 - \alpha)$ then after executing $\log n$ -A3F for vertices as described above on $G = (V, E)$ we obtain $G_A = (V \setminus W, (E \cup E_P) \setminus E_C)$ which is whp $(1 - (1 - \beta)\alpha)$ -strong.

Proof. Let \tilde{N}_W denote the set of vertices from N_W which take part in the protocol ($|\tilde{N}_W| = \gamma|N_W|$). Even though the vertices from $N_W \setminus \tilde{N}_W$ do not take part in the protocol, they can be chosen as those to whom vertices from \tilde{N}_W establish new edges. Let us estimate the probability that $v \in N_W \setminus \tilde{N}_W$ will not get connected to any vertex from \tilde{N}_W during the execution of the protocol (denote this event by $[v \not\leftrightarrow G(\tilde{N}_W)]$). Let i be such that w_i and v are neighbors in G . We have

$$\begin{aligned}
\mathbb{P}[v \not\leftrightarrow G(\tilde{N}_W)] &\leq \left(1 - \frac{1}{C \log n \deg(w_i)}\right)^{\gamma|N_W| \log n} \leq \\
&\left(1 - \frac{1}{Cbn}\right)^{\gamma|N_W| \log n} \leq e^{-(\gamma \log n |N_W|)/(Cbn)} = \\
&n^{-\gamma(1-\alpha)/(Cb)} n^{\log n/(bn)}
\end{aligned}$$

(compare 1).

Now, let us estimate the probability that all vertices from $(N_W \setminus \tilde{N}_W)$ are going to be connected with $G(\tilde{N}_W)$ (denote this event by $[(N_W \setminus \tilde{N}_W) \leftrightarrow G(\tilde{N}_W)]$). We get

$$\begin{aligned} \mathbb{P}[(N_W \setminus \tilde{N}_W) \leftrightarrow G(\tilde{N}_W)] &\geq \\ &\left(1 - n^{-\gamma(1-\alpha)/(Cb)} n^{\log n/(bn)}\right)^{(1-\gamma)|N_W|} = \\ &\left(1 - n^{-\gamma(1-\alpha)/(Cb)} n^{\log n/(bn)}\right)^{(1-\gamma)((1-\alpha)n - C \log n)} \\ &\xrightarrow{n \rightarrow \infty} 1 \end{aligned}$$

since $Cb > \gamma(1-\alpha)$. Thus again whp $G(N_W)$ is connected.

By calculations analogous to those from Theorem 1 we also get that all vertices from V_α which participate in the protocol (denote this set by \tilde{V}_α) are connected with $G(N_W)$ whp. We proved that whp G_A has a giant component containing $N_W \cup \tilde{V}_\alpha$, $|N_W \cup \tilde{V}_\alpha| = (1-\alpha)n - C \log n + \beta \alpha n$. This completes the proof. \square

V. EXPERIMENTAL RESULTS

We present experimental results conducted on **real** data of Epinions social network collected in SNAP dataset by Stanford University (see [17] and [18]).

This is a who-trust-whom online social network of a general consumer review site Epinions.com. Members of the site can decide whether to "trust" each other. All the trust relationships interact and form the Web of Trust which is then combined with review ratings to determine which reviews are shown to the user. Our network has 75879 nodes and 508837 edges where nodes denote users of Epinions.com site and edges denote trust relation.

A. Random Failures

Random failures is a widely used model in network robustness but also fault tolerance (see [19]) literature. We assume that corrupted nodes (or in other words, nodes which are prone to failure) are distributed in a uniform way across the whole network.

1) *m-2SFF Protocol*: First let us concentrate on the *m-2SFF* Protocol in the case of Random Failures. Initially we assume that all nodes launch the *m-2SFF* Protocol, namely each node does *m* random walks of length 2 to establish extra connections. Obviously, the larger *m*, the better safety of the nodes.

In Figure 1 we show how the *m-2SFF* Protocol performs on Epinions social network graph under Random Failures model. We can see how the network behaves without any enrichment, and with $m = 1, 5, 10, 15$. Note that on the x-axis we have the percentage of corrupted nodes. With $m = 15$ walks, around 70% of remaining nodes are in the single **giant** connected component. Note that the edges are added **before** the corruption phase. Therefore, for each remaining node, a lot of added neighbors are corrupted and therefore useless. On the positive side, one can easily see that for up to around 20% failures, even 5 walks are sufficient to have almost every node belonging to the giant component.

Despite these somewhat optimistic results, it is quite unrealistic to assume that all users want to participate. We want to weaken this assumption. We still demand high level of security, at least for the participating users. In the Figure 2 we show some experimental results when a part of nodes participates, only. Here we assume $m = 15$ and $q = 0.1, 0.25, 0.5$ fraction of participating nodes. That is, $q \cdot n$ nodes participate in 15-2SFF protocol. Then we are interested what is the fraction of participating users that belong to the biggest

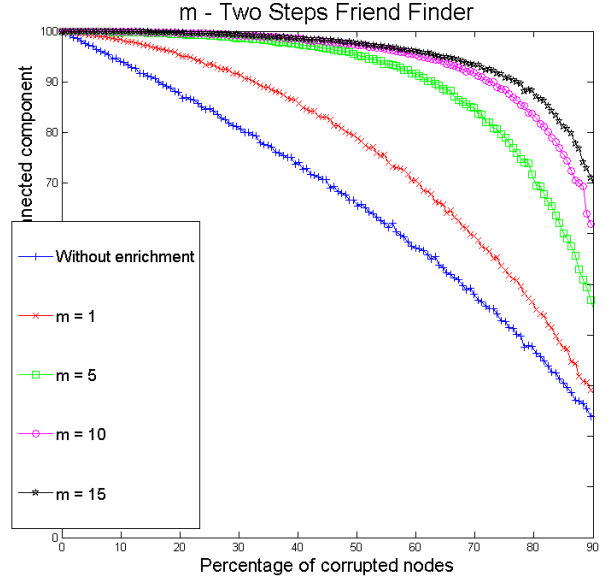


Fig. 1: *m-2SFF* under Random Failures model.

component and how it compares to the situation when all users do participate.

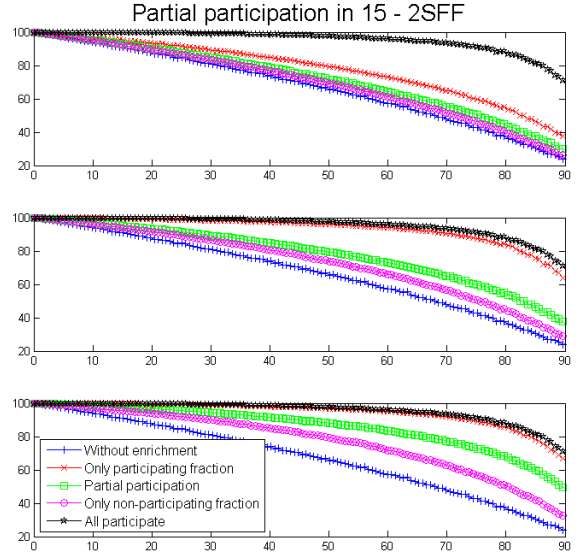


Fig. 2: 15-2SFF under Partial Participation and Random Failures model. The top figure shows 10% participation, middle shows 25% participation and bottom 50% participation.

Note that in the case where $q = 0.1$ there is a significant decrease of security. Namely, with massive number of failures, we have around 30% nodes in biggest component in comparison to 70% in the full participation case. Note that even if we consider only the subset of participating nodes, then the fraction of nodes belonging to biggest component amongst them is below 40%. The security indeed improves with greater q , yet still even if we consider only the participating nodes, the results are significantly worse than

when all users participate. Thus this protocol turned to be useful in communities if we know that strong majority of nodes is willing to use it.

2) *m-A3F Protocol*: Now we focus on the *m-A3F* protocol under Random Failures model. Again, we initially assume that all nodes participate in the protocol, namely each node does m queries which consist of randomly choosing one of the fat nodes and asking for randomly chosen neighbor of that node. Here we fixed the number of the nodes considered fat for $\lfloor \log(n) \rfloor = 16$. It means that 16 nodes which have the highest degree in the initial graph are on the common list of 'fat nodes'.

In Figure 3 one can see the performance of A3F on Epinions social network graph under Random Failures model. Similarly as before, we show the behavior of the network without any enrichment, and with $m = 1, 5, 10, 15$. This time, with $m = 15$ queries, almost 90% of remaining nodes are in the giant component despite of a large number of failures. Another interesting thing to observe is that the cutoff (moment when the fraction of nodes in the giant component begins to decrease significantly) appears much farther. For example, in case of 15-2SFF we see that the size of the giant component starts to deteriorate since approximately 30% failures, before this threshold it remains very close to 100%. In the case of 2SFF, on the other hand, for $m = 15$ the cutoff appears as far as 70% failures and before such a massive corruption of nodes, it remains negligibly close to 100%.

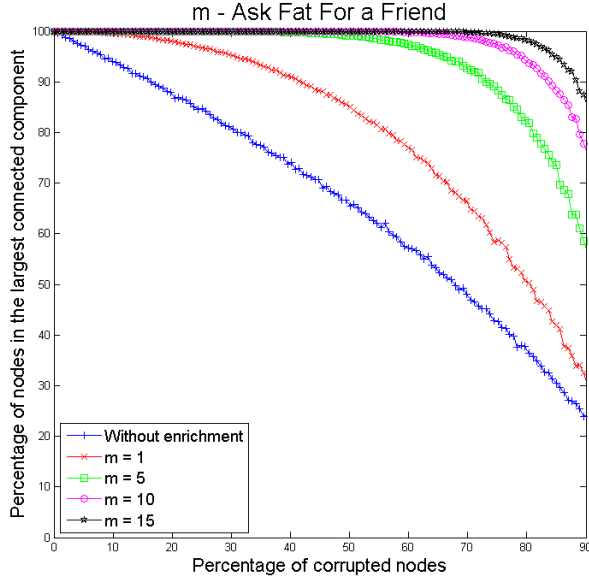


Fig. 3: *m-A3F* under Random Failures model.

Again we are interested in the performance of A3F in the case where only a fraction of users wants to participate. We assumed $m = 15$ and $q = 0.1, 0.25, 0.5$ participation. In Figure 4 we have shown the results for 2SFF with partial participation.

The most interesting thing is the fact that the safety level amongst the participating nodes in case of partial participation is virtually the same as the safety level when all nodes participate. This fact is very important from the practical point of view. It gives the users a choice - whether they want to sacrifice their safety and not participate in the protocol, or participate in the protocol and be safe no matter what other users choose as long as at least some fraction (say 10%) decides to participate in the protocol.

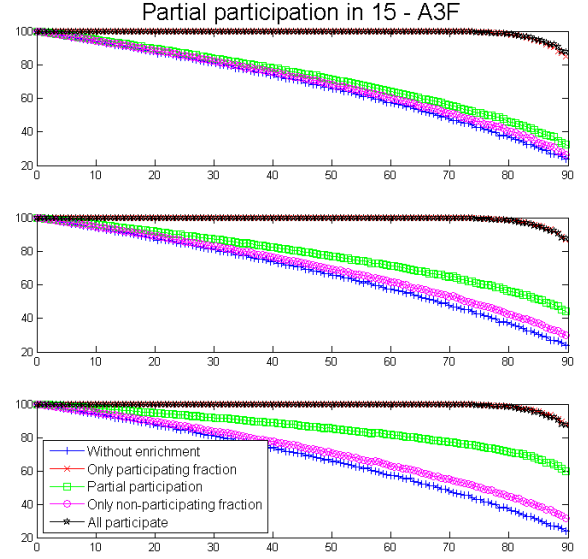


Fig. 4: 15-A3F under Partial Participation and Random Failures model. The top figure shows 10% participation, middle shows 25% participation and bottom 50% participation.

3) *Comparison*: A glance at the figures in this subsection is enough to see that *m-A3F* performs better than *m-2SF* under Random Failures regime. See for example that for $m = 10$ and for 90% failures the A3F protocol gives approximately 80% nodes belonging to the giant component, while 2SFF gives only 60%. Moreover, for the cutoff and therefore non-negligible deterioration of the fraction of nodes in the biggest component appears for greater fraction of failures than in *m-2SF* protocol.

Intuitively, these differences in the results stem from the fact that in A3F we leverage naturally emerging preferential attachment models in real, complex networks, while 2SFF does not really utilize this fact. Connecting to neighbors of fixed, high-degree set of nodes massively improves robustness of real networks.

B. Targeted Adversary

In this subsection we present experiments conducted under far stronger Adversary that can corrupt nodes of the highest degree. Namely, if the Adversary has to corrupt k nodes, she sorts the list of nodes by degree and corrupts first k of them.

Note that the Adversary only has access to the initial graph, without enrichment. Obviously, for a specific instance of the graph one could possibly devise a more clever way of attack, however this strategy seems to be optimal in general. Note that complex network which resemble preferential attachment features are extremely prone to such attacks.

1) *m-2SFF protocol*: In Figure 5 we show how *m-2SFF* performs on Epinions social network graph under Targeted Adversary model. We can see how the network behaves without any enrichment, and with $m = 1, 5, 10, 15$. Note that on the x-axis we have the percentage of corrupted nodes and this time it ranges from 0 to 30% instead of 0–90% due to the Adversary's strength. Note that without enrichment the fraction of nodes in the biggest² component dramatically falls to

²Note that from graph-theory perspective we have in this case a *giant component* - a single component that contains a fraction of all nodes

almost 0 for 20% failures. In other words, if the Adversary destroys 20% nodes of highest degree, the remaining graph consists only of very small components. On the other hand, see that for up to 5% corruptions the $m = 15$ walks version gives almost 100% nodes belonging to the biggest component. Even for 30% corruption the fraction of nodes in the biggest component is considerably large (approximately 60%). Recall that without enrichment under such a strong adversary there is virtually no giant component whatsoever.

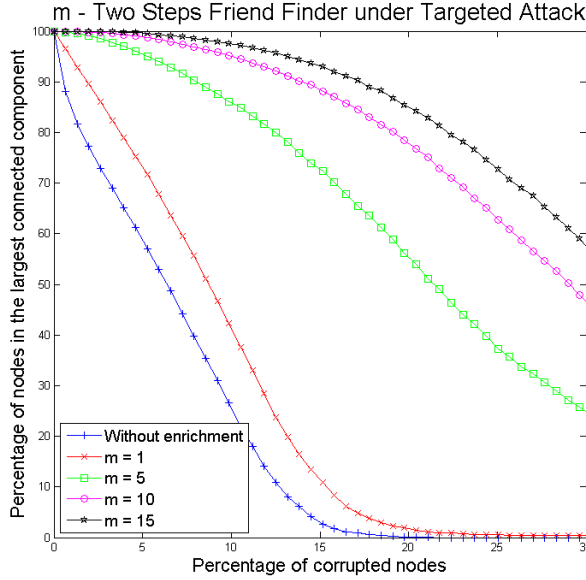


Fig. 5: m -2SFF under Targeted Attack.

Let us investigate the protocol if we assume that only a fraction of non-corrupted users participate actively. We assumed $m = 15$ and $q = 0.1, 0.25, 0.5$ participation. In Figure 6 we have shown the results for m -2SFF with partial participation under Targeted Adversary regime.

An interesting difference between the results for this model and Random Failures can be seen in this figure. Namely, the fraction of nodes belonging to the giant component amongst those who participate is only slightly greater than amongst those who do not participate. This is highly undesired, as it gives no notion of improvement and benefit of participating actively in the protocol. A node could decide that it is pointless to waste precious resources and rather hope that the others would participate actively. See that even if half of the users actively participate, the fraction of nodes in the giant component are significantly smaller than when all nodes participate.

2) m -A3F protocol: After somewhat unsatisfying results for m -2SFF under Targeted Adversary, we will now present experiments on the m -A3F protocol. As before, let us first assume that all nodes participate in the protocol.

In Figure 7 one can see the performance of m -A3F on Epinions social network graph under Targeted Adversary model. As previously, we show the behavior of the network without any enrichment, and for the cases where $m = 1, 5, 10, 15$. This time, with $m = 15$ queries, approximately 85% of remaining nodes are in the biggest component for up to 30% corruptions and over 95% of nodes are in the giant component for up to 15% corruptions. Another interesting thing to observe is that the cutoff again appears for greater number of corruptions. For example, in case of 15-2SFF we see that the size

Partial participation in 15-2SFF under Targeted Attack

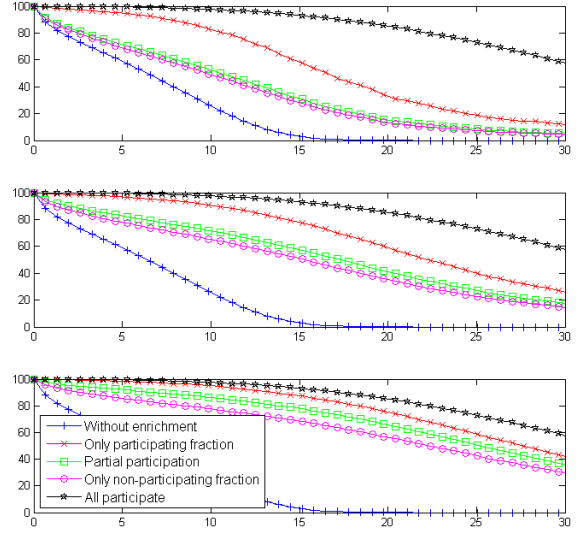


Fig. 6: Partial 15-2SFF under Targeted Attack. The top figure shows 10% participation, middle shows 25% participation and bottom 50% participation.

of the giant component starts to deteriorate since approximately 5% failures, before this threshold it remains close to 100%. In the case of 15-A3F, on the other hand, the cutoff appears as far as at 10% failures.

15 - Ask Fat For a Friend under Targeted Attack

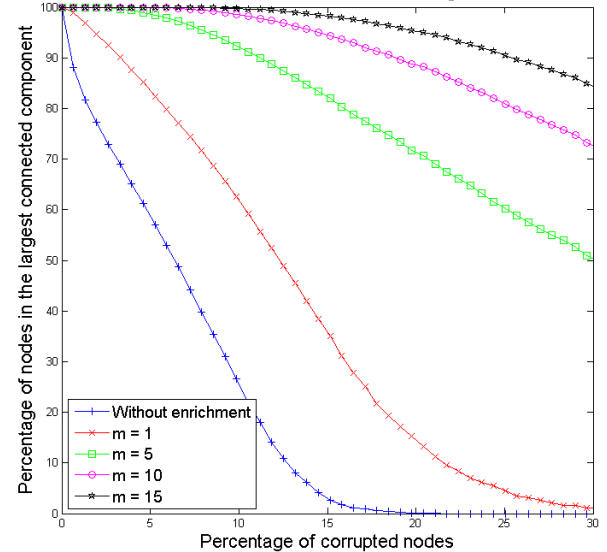


Fig. 7: m -A3F under Targeted Attack.

Similarly as in the previous subsection, we want to see how the protocol behaves if we assume that only a fraction of non-corrupted users participate actively. We assumed $m = 15$ and $q = 0.1, 0.25, 0.5$ participation. In Figure 8 we show the results for A3F with partial participation under Targeted Adversary regime.

Partial participation in 15 - A3F under Targeted Attack

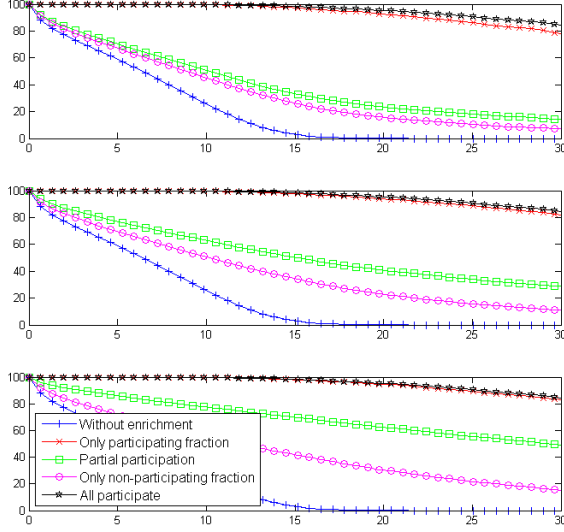


Fig. 8: Partial 15-A3F under Targeted Attack. The top figure shows 10% participation, middle shows 25% participation and bottom 50% participation.

Figure 8 is probably the most striking one due to the fact that in all three cases, one can easily see that the fraction of nodes belonging to the giant component amongst the actively participating nodes is almost the same as when all nodes participate. This is a **very desirable** feature of m -A3F because it gives the user a natural choice - participate in the protocol, which costs some computational resources, but be in the giant component independently of the choices of other nodes or do not participate, but then you are facing serious risk of ending up disconnected from the giant component.

3) *Comparison*: First of all, the results for both protocols are obviously worse than for Random Failure model, which is not surprising. However, they still give a significant improvement of the size of the giant component. Moreover, in the regime of Targeted Adversary, the m -A3F has a very interesting property of assuring almost the same fraction of nodes belonging to the giant component for participating fraction of nodes (even if only 10% of users participate) as in the case where all users participate.

This regime shows that m -A3F is indeed a very powerful enrichment to the graph structure. Note that we went from no giant component for 20% failures to almost 90% nodes belonging to the giant component amongst the actively participating nodes even if only 10% of users participate. This scenario shows a significant improvement of security which is gained via m -A3F for those who actively participate in it. Note that the difference between the performance of m -2SFF and m -A3F is strongly connected with utilizing preferential attachment in real networks.

VI. SOME CONSEQUENCES FOR SECURITY AND PRIVACY

Let us assume that graph G is ξ -strong.

Corollary 1: Assume that we have a network with underlying graph G which is ξ -strong. Then using cryptographic methods for data aggregation (see for example [10]) one can aggregate data even without adding noise. Such results are already presented in literature and require appropriate amount of users participating (see [20], [21], [22])

Corollary 2: Assume that we have a network with underlying graph G which is ξ -strong. Then aggregation protocol PAALEC from [23] with parameters $\alpha = \exp(-\frac{\epsilon}{\Delta})$ and $\beta = \frac{2\log(1/\delta)}{s}$ applied to graph G is (ϵ, δ) -differentially private for the nodes belonging to the largest connected component. Moreover, PAALEC aggregation protocol is $(\epsilon, \delta + (1 - \xi))$ -differentially private for any arbitrary node.

VII. PREVIOUS AND RELATED WORK

This paper spans several areas, thus many different papers should be pointed as related work. Since the idea of scale free network modeling appeared, there has been a vast amount of research concerning these kind of networks, including classic papers like [24], [25], [26], [27], [28]. Also worth mentioning are papers which provided rigorous mathematical treatment for scale free networks [29], [30], [31]. More recent papers on properties of scale free networks include [32], [33]. Also worth mentioning are papers [34], [35] where authors consider various properties of a graph given its expected degree list.

We should also mention papers about community structure in large networks [36], [37]. Some empirical result can also be found in [38].

The problem of robustness in complex networks has also been widely analyzed. To mention a few papers concerning the robustness and enhancing of robustness in scale free networks we cite [15], [39], [13], [40]. One should also mention [41] wherein authors consider adversarial deletion in scale free graphs and [12], where authors improve graph robustness by edge modifications. Note that, in the network robustness literature the notion of robustness is mostly the fact that the largest connected component exists. Here, however, we are interested in non-asymptotic results and more precise size (or lower bound for the size) of the giant component. Moreover, our protocols can be performed locally and without knowledge of the graph topology.

Furthermore, papers concerning various anonymity and 'crowd-blending' concepts should be mentioned. See for example [1], [8], [7], [3], [4] for k -anonymity. See also [5], [6] for extensions and variations of anonymity.

We should also mention some privacy preserving papers with emphasis on those which could benefit from having large connected component of appropriate size, namely [20], [21], [22], [23]. Also important are the papers [10], [19] where authors use cryptographic methods to amplify privacy for large group of users in data aggregation scenario. For survey about privacy see [42] and references therein.

VIII. CONCLUSIONS AND FUTURE WORK

We presented how to improve the size of the largest connected component under massive adversarial attack and demonstrated why this observation is important for a wide range of applications (with most emphasis put on privacy preserving protocols). Moreover, our methods are conceptually simple and can be performed locally, i.e. with minimal knowledge about the global network. We proved that the presented methods are efficient in preferential-attachment graphs, which are commonly believed to be an accurate model of various real-life networks including social interaction networks, World Wide Web, airline networks and many other. Finally, we confirmed our observations using experiments on graphs of **real** networks.

We believe that many questions important both for theory as well as design of practical privacy preserving solutions are left unanswered. In particular, for future work we plan to investigate:

- even stronger Adversary, who can choose adaptively (namely during the enhancement protocol) vertices to corrupt;

- longer random walks, where we establish an edge with every node visited on the way;
- Our protocols improve security of participating individuals, but the level of privacy is improved also for other users. The question is, how to design a mechanism (i.e., via constructing extra incentives) to improve global privacy dependently on a power of the adversary.

REFERENCES

- [1] A. Pfitzmann and M. Kohntopp, "Anonymity, unobservability, and pseudonymity - A proposal for terminology," in *Designing Privacy Enhancing Technologies, International Workshop on Design Issues in Anonymity and Unobservability*, Berkeley, CA, USA, July 25-26, 2000, *Proceedings*, ser. Lecture Notes in Computer Science, H. Federrath, Ed., vol. 2009. Springer, 2000, pp. 1-9. [Online]. Available: http://dx.doi.org/10.1007/3-540-44702-4_1
- [2] P. Samarati, "Protecting respondents identities in microdata release," *IEEE transactions on Knowledge and Data Engineering*, vol. 13, no. 6, pp. 1010-1027, 2001.
- [3] P. Samarati and L. Sweeney, "Generalizing data to provide anonymity when disclosing information," in *Proceedings of the seventeenth ACM SIGACT-SIGMOD-SIGART symposium on Principles of database systems*, ser. PODS '98, 1998, p. 188.
- [4] L. Sweeney, "k-anonymity: a model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, pp. 557-570, 2002.
- [5] A. Machanavajhala, J. Gehrke, D. Kifer, and M. Venkatasubramanian, "l-diversity: Privacy beyond κ -anonymity," in *Proceedings of the 22nd International Conference on Data Engineering*, ser. ICDE '06, 2006, p. 24.
- [6] X. Xiao and Y. Tao, "M-invariance: towards privacy preserving re-publication of dynamic datasets," in *Proceedings of the 2007 ACM SIGMOD international conference on Management of data*, ser. SIGMOD '07, 2007, pp. 689-700.
- [7] C. Díaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity," in *Privacy Enhancing Technologies, Second International Workshop, PET 2002, San Francisco, CA, USA, April 14-15, 2002, Revised Papers*, 2002, pp. 54-68. [Online]. Available: http://dx.doi.org/10.1007/3-540-36467-6_5
- [8] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity," in *Privacy Enhancing Technologies, Second International Workshop, PET 2002, San Francisco, CA, USA, April 14-15, 2002, Revised Papers*, 2002, pp. 41-53. [Online]. Available: http://dx.doi.org/10.1007/3-540-36467-6_4
- [9] C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*, ser. Lecture Notes in Computer Science, S. Halevi and T. Rabin, Eds., vol. 3876. Springer, 2006, pp. 265-284. [Online]. Available: http://dx.doi.org/10.1007/11681878_14
- [10] E. Shi, R. Chow, T. h. Hubert Chan, D. Song, and E. Rieffel, "Privacy-preserving aggregation of time-series data," in *IN NDSS*, 2011.
- [11] V. Rastogi and S. Nath, "Differentially private aggregation of distributed time-series with transformation and encryption," in *Proceedings of the 2010 ACM SIGMOD International Conference on Management of Data*, ser. SIGMOD '10. New York, NY, USA: ACM, 2010, pp. 735-746. [Online]. Available: <http://doi.acm.org/10.1145/1807167.1807247>
- [12] A. Beygelzimer, G. Grinstein, R. Linsker, and I. Rish, "Improving network robustness by edge modification," *Physica A: Statistical Mechanics and its Applications*, vol. 357, no. 3, pp. 593-612, 2005.
- [13] H. Zhang, E. Fata, and S. Sundaram, "A notion of robustness in complex networks," *IEEE Transactions on Control of Network Systems*, vol. 2, no. 3, pp. 310-320, 2015.
- [14] D. S. Callaway, M. E. Newman, S. H. Strogatz, and D. J. Watts, "Network robustness and fragility: Percolation on random graphs," *Physical review letters*, vol. 85, no. 25, p. 5468, 2000.
- [15] J. Zhao and K. Xu, "Enhancing the robustness of scale-free networks," *Journal of Physics A: Mathematical and Theoretical*, vol. 42, no. 19, p. 195003, 2009.
- [16] B. Bollobás, "Random graphs," in *Modern Graph Theory*. Springer, 1998, pp. 215-252.
- [17] J. Leskovec and A. Krevl, "SNAP Datasets: Stanford large network dataset collection," <http://snap.stanford.edu/data>, Jun. 2014.
- [18] M. Richardson, R. Agrawal, and P. Domingos, "Trust management for the semantic web," in *International semantic Web conference*. Springer, 2003, pp. 351-368.
- [19] T.-H. H. Chan, E. Shi, and D. Song, "Privacy-preserving stream aggregation with fault tolerance," in *Financial Cryptography*, ser. Lecture Notes in Computer Science, A. D. Keromytis, Ed., vol. 7397. Springer, 2012, pp. 200-214. [Online]. Available: <http://dblp.uni-trier.de/db/conf/fc/fc2012.html#ChanSS12>
- [20] R. Bassily, A. Groce, J. Katz, and A. Smith, "Coupled-worlds privacy: Exploiting adversarial uncertainty in statistical data privacy," in *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*. IEEE, 2013, pp. 439-448.
- [21] R. Bhaskar, A. Bhowmick, V. Goyal, S. Laxman, and A. Thakurta, "Noiseless database privacy," in *International Conference on the Theory and Application of Cryptology and Information Security*. Springer, 2011, pp. 215-232.
- [22] D. Kifer and A. Machanavajhala, "A rigorous and customizable framework for privacy," in *Proceedings of the 31st ACM SIGMOD-SIGACT-SIGAI symposium on Principles of Database Systems*. ACM, 2012, pp. 77-88.
- [23] K. Grining, M. Klonowski, and P. Syga, "Practical fault-tolerant data aggregation," in *International Conference on Applied Cryptography and Network Security*. Springer, 2016, pp. 386-404.
- [24] R. Albert and A.-L. Barabási, "Statistical mechanics of complex networks," *Reviews of modern physics*, vol. 74, no. 1, p. 47, 2002.
- [25] A.-L. Barabási and E. Bonabeau, "Scale-free networks," *Scientific American*, vol. 288, no. 5, pp. 50-59, 2003.
- [26] R. Kumar, P. Raghavan, S. Rajagopalan, D. Sivakumar, A. Tomkins, and E. Upfal, "Stochastic models for the web graph," in *Foundations of Computer Science, 2000. Proceedings. 41st Annual Symposium on*. IEEE, 2000, pp. 57-65.
- [27] W. Aiello, F. Chung, and L. Lu, "A random graph model for massive graphs," in *Proceedings of the thirty-second annual ACM symposium on Theory of computing*. AcM, 2000, pp. 171-180.
- [28] S. H. Strogatz, "Exploring complex networks," *Nature*, vol. 410, no. 6825, pp. 268-276, 2001.
- [29] B. Bollobás, O. Riordan, J. Spencer, G. Tusnády et al., "The degree sequence of a scale-free random graph process," *Random Structures & Algorithms*, vol. 18, no. 3, pp. 279-290, 2001.
- [30] B. Bollobás and O. M. Riordan, "Mathematical results on scale-free random graphs," *Handbook of graphs and networks: from the genome to the internet*, pp. 1-34, 2003.
- [31] B. Bollobás and O. Riordan, "The diameter of a scale-free random graph," *Combinatorica*, vol. 24, no. 1, pp. 5-34, 2004.
- [32] A.-L. Barabási, "Scale-free networks: a decade and beyond," *science*, vol. 325, no. 5939, pp. 412-413, 2009.
- [33] B. Fotouhi and M. G. Rabbat, "Degree correlation in scale-free graphs," *arXiv preprint arXiv:1308.5169*, 2013.
- [34] F. Chung and L. Lu, "Connected components in random graphs with given expected degree sequences," *Annals of combinatorics*, vol. 6, no. 2, pp. 125-145, 2002.
- [35] —, "The average distance in a random graph with given expected degrees," *Internet Mathematics*, vol. 1, no. 1, pp. 91-113, 2004.
- [36] J. Leskovec, K. J. Lang, A. Dasgupta, and M. W. Mahoney, "Community structure in large networks: Natural cluster sizes and the absence of large well-defined clusters," *Internet Mathematics*, vol. 6, no. 1, pp. 29-123, 2009.
- [37] R. Van Der Hofstad, "Random graphs and complex networks," Available on <http://www.win.tue.nl/rhofstad/NotesRGCN.pdf>, p. 11, 2009.
- [38] A. Clauset, C. R. Shalizi, and M. E. Newman, "Power-law distributions in empirical data," *SIAM review*, vol. 51, no. 4, pp. 661-703, 2009.
- [39] G. Tanaka, K. Morino, and K. Aihara, "Dynamical robustness in complex networks: the crucial role of low-degree nodes," *Scientific reports*, vol. 2, p. 232, 2012.
- [40] Y. Yang, Z. Li, Y. Chen, X. Zhang, and S. Wang, "Improving the robustness of complex networks with preserving community structure," *PloS one*, vol. 10, no. 2, p. e0116551, 2015.
- [41] A. D. Flaxman, A. M. Frieze, and J. Vera, "Adversarial deletion in a scale free random graph process," in *Proceedings of the sixteenth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics, 2005, pp. 287-292.
- [42] C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211-407, 2014.